

EXHIBIT 41



NVD MENU

NATIONAL VULNERABILITY DATABASE

NVD

800-53/800-53A

REV4

NIST Special Publication 800-53 (Rev. 4)

Security and Privacy Controls for Federal Information Systems and Organizations

AC-11 SESSION LOCK

Family: AC - ACCESS CONTROL

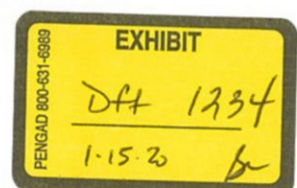
Class:

Priority: P3 - Implement P3 security controls after implementation of P1 and P2 controls.

Baseline Allocation:	Low	Moderate	High
	N/A	AC-11 (1)	AC-11 (1)

Jump To:

Revision 4 Statements
Control Description
Supplemental Guidance
References

All Controls > AC > **AC-11**

Control Description

The information system:

- a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and
- b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.

Related to: AC-7

Control Enhancements

AC-11(1) SESSION LOCK | PATTERN-HIDING DISPLAYS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

References

OMB <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-16.pdf>
Memorandum 16.pdf
06-16

800-53 (Rev. 4)

Security Controls

Low-Impact

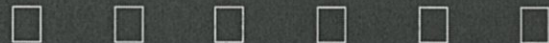
Moderate-Impact

High-Impact

Other Links

Families

Search



HEADQUARTERS

100 Bureau Drive
Gaithersburg, MD 20899

[Webmaster](#) | [Contact Us](#) | [Our Other Offices](#)

GENERAL

[NVD Dashboard](#)

[News](#)

[Email List](#)

[FAQ](#)

[Visualizations](#)

VULNERABILITIES

[Search & Statistics](#)

[Full Listing](#)

[Categories](#)

[Data Feeds](#)

[Vendor Comments](#)

VULNERABILITY METRICS

[CVSS V3 Calculator](#)

[CVSS V2 Calculator](#)

PRODUCTS

[CPE Dictionary](#)

Information Technology Laboratory (ITL) National Vulnerability Database (NVD)

[Announcement and Discussion Lists](#)

General Questions & Webmaster Contact

Email: nvd@nist.gov

Incident Response Assistance and Non- NVD Related Technical Cyber Security

Questions:

[US-CERT Security Operations Center](#)

Email: soc@us-cert.gov

Phone: 1-888-282-0870

Sponsored by
DHS/NCCIC/US-CERT



[CPE Search](#)

[CPE Statistics](#)

[SWID](#)

[CONFIGURATIONS \(CCE\)](#)

[CONTACT NVD](#)

[OTHER SITES](#)

[Checklist \(NCP\) Repository](#)

[800-53 Controls](#)

[SCAP Validated Tools](#)

[SCAP](#)

[USGCB](#)

[SEARCH](#)

[Vulnerability Search](#)

[CPE Search](#)

[Privacy Statement](#) | [Privacy Policy](#) | [Security Notice](#) | [Accessibility Statement](#) | [NIST Privacy Program](#) | [No Fear Act Policy](#)

[Disclaimer](#) | [FOIA](#) | [Environmental Policy Statement](#) | [Cookie Disclaimer](#) | [Scientific Integrity Summary](#) | [NIST Information Quality Standards](#)

[Business USA](#) | [Healthcare.gov](#) | [Science.gov](#) | [USA.gov](#)